Coinmonks

Bitcoin + Cryptocurrencie + Forensics + Analytics + Blockchain +

Free Bitcoin Forensics - Part 1

Pagan Follow 14 min read · Dec 10, 2020

75

In the past few years, Bitcoin forensics and privacy has attracted more and more attention and controversy in Bitcoin and the wider crypto ecosystem. With the rise of sophisticated privacy tools such as Coinjoin wallets like Wasabi, Samourai, and Joinmarket as well as sophisticated adversaries (such as Chainalysis and law enforcement) it is fair to say that that the field has advanced quite a bit and continues to advance at a breakneck speed. In this article, I wish to explore how far can we push Bitcoin analytics while not using any paid advanced tools and not having any coding skills or degrees in mathematics. In short, just how much a (relatively) less technical, but very determined Bitcoin user can understand from the bitcoin blockchain. I hope this blog post teaches you not only how bitcoin forensics can be conducted but also what mistakes can be avoided to preserve privacy.

This blog post will be split into 3 parts, in the first one I will be explaining the very basics of Bitcoin analytics, in the second we will delve deeper and explore Bitcoin analytics from a more technical side (still no programming skills required), finally in the third part we will conduct a mock investigation to put some of the information here into practice.

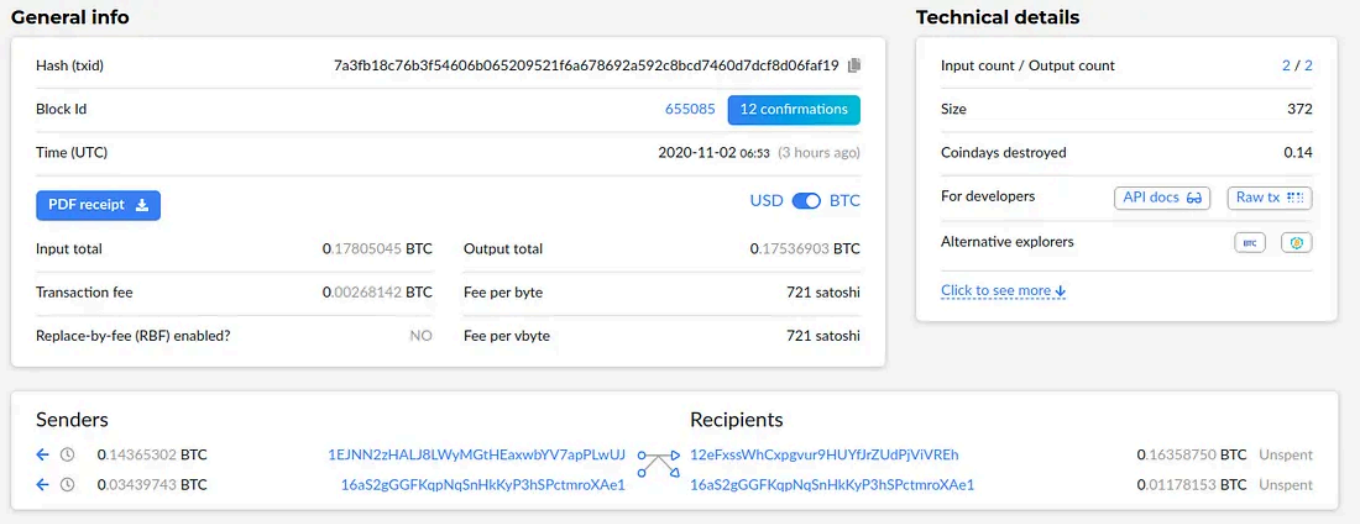
Before I begin, I must mention, that, despite its length, this blog post is in no way a comprehensive overview of Bitcoin forensics, the truth is, Bitcoin forensics is a very expansive science in itself and it keeps growing. This article was written in December 2020, so some parts of it will inevitably become outdated as time goes on.

Finally, before starting I must note that you need to have a good understanding of Bitcoin transactions to get the most out of this blog. If you haven't already, I'd recommend checking out the transactions chapter of the "Mastering Bitcoin" book (or just check out the whole book, it's a great one,

plus it's free):
https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch06.asciidoc

The Individual Transaction Basics

To begin with, let's get introduced to basic Bitcoin transactions and the basic conclusions we can draw from them. The usual transaction you will encounter while exploring the blockchain will look something like this:



https://blockchair.com/bitcoin/transaction/7a3fb18c76b3f54606b065209521f6a678692a592c8bcd7460d7dcf8d06faf19

Already we have a lot of information about the transaction, such as the time when it happened, the fee, addresses involved, the size of the transaction and so much more! But we will discuss the implications of having all of this metadata a bit later, for now, let's look at what we can reason just from the Senders/Recipient (commonly referred to as inputs/outputs) part:

Just from this, we can make several important conclusions:

1. All the sender addresses belong to the same person/entity.

Unless this transaction is a Coinjoin or Payjoin (and it doesn't look like a Coinjoin and is very unlikely to be a Payjoin) all of the sender (input) addresses belong to the same entity. This is a very safe assumption to make that as the vast majority of inputs in Bitcoin transactions belong one entity. Coinjoins and Payjoins break this assumption on purpose to improve the privacy of the senders, but payjoins are very rare and Coinjoins are quite easy to recognize.

2. This transaction has a change address (and it starts with 16a…).

The second important assumption we can make is that this transaction has a change address that also belongs to the sender. In this case, we are immediately able to say that the change address is the one that starts with 16a as this address also appears on the input side, in other transactions, the change address may be less obvious, but there are many other indications that may help you to determine the change address.

3. The address that starts with 12e is the destination address.

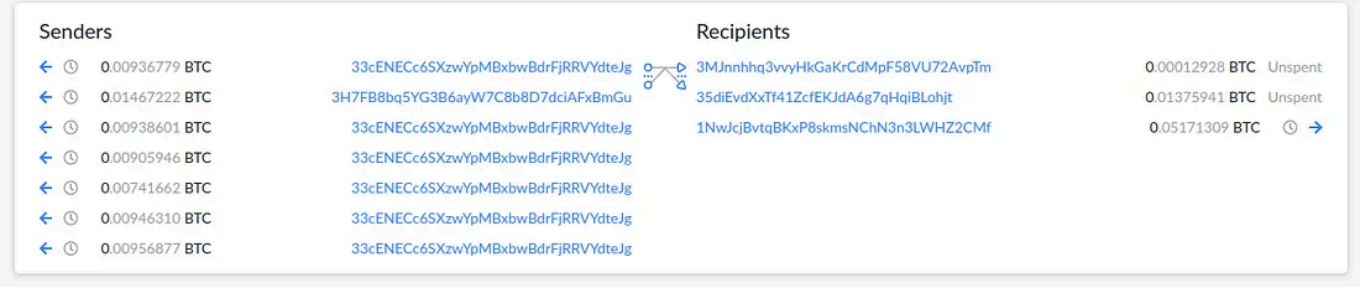
Since we know that address that starts with 16a is a change address that means that the address which starts with 12e can only be the destination address. To which the sender wishes to transfers part of their coins (0.16358750 BTC to be exact). Now, of course, we can't really say if this address belongs to someone else or is the sender's address in another wallet that they also control, but we can say that this is the only address that realistically may not belong to the sender.

Having made all these assumptions we can color the transaction to signify ownership, where the addresses marked in red belong to the sender and the address marked in yellow belong to the recipient:

Although this is one of the most common and basic compositions of transactions you can encounter, this, of course, is far from the only type of transaction out there. Transactions can come in all shapes and sizes, there really isn't much that is limiting the number of inputs and outputs a transaction can have. To illustrate this, I've randomly picked some transactions from a random block, let's see what we can determine from them:

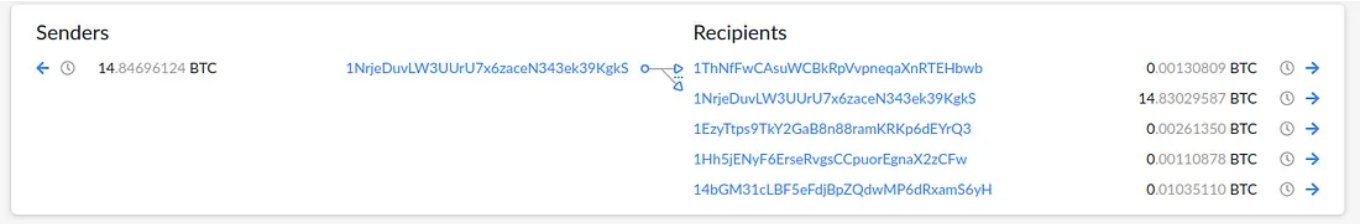
https://blockchair.com/bitcoin/transaction/0ec7de5b781fe8bff7638dca5f40e8d157287ed83496ae96b430d34c12ec8490

This transaction lacks any change address which makes it quite likely to be a "sweep", meaning that all the funds from the sender addresses were transferred to another address which is likely also controlled by the sender. Once we check the sender addresses we do in-fact see that they do not have any funds in them left, which makes the assumption more likely.



https://blockchair.com/bitcoin/transaction/941b29236d767bd7bbc61c85574c891c18ac4ea5f514c0e76f38a3507fde9c0c

In this transaction, we can assume that the change address is one of the two addresses that start with 3 (this address type is called Pay-to-Script-Hash or P2SH) in the recipient's section while the destination address is the one that starts with 1 (this address type is called Pay-to-Public-Key-Hash or P2PKH). Crypto wallets rarely create a different type of address for change, usually, the change address and the input is the same type. Determining which of the addresses that start with 3 is the actual change address is much harder, however.

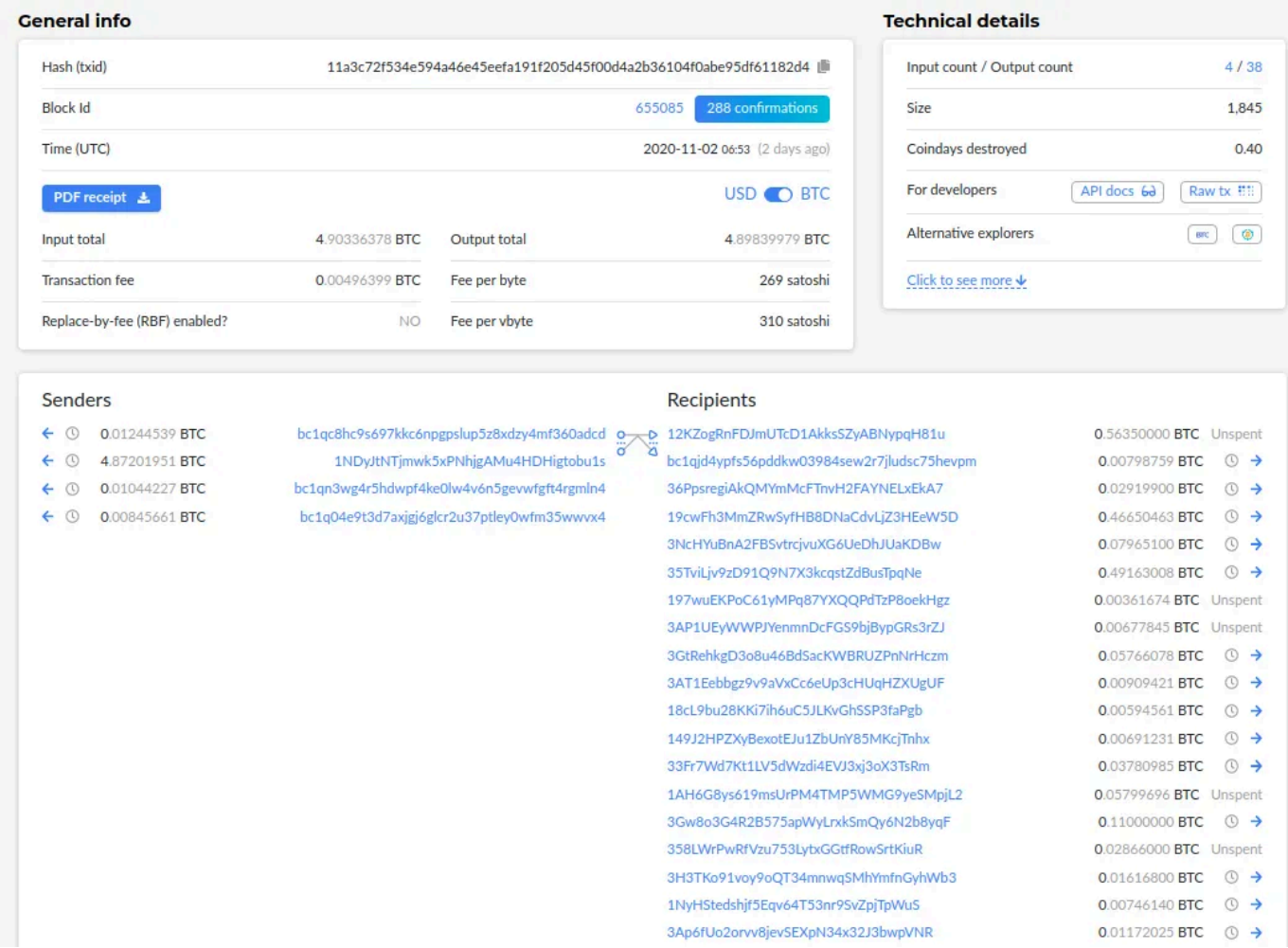


https://blockchair.com/bitcoin/transaction/5d3c39bbd3d606c43e9146dcbf41d1d93b70023b68bf818e46b23fe71744bcaf

This transaction doesn't suffer from the use of multiple address types, but since the input address is the same as one of the outputs it makes it very obvious which is the change address. Without address reuse this transaction would be perfectly private (well, if you also exclude the fact that the change output is so much bigger than all the outputs, which is also a clue). Address reuse is one of the gravest sins one can commit to compromise their privacy.

These sort of “few inputs, few outputs” transactions are the most common in the blockchain, however, there are 2 other types of transactions worth knowing about:

> *Exchange transactions*



https://blockchair.com/bitcoin/transaction/11a3c72f534e594a46e45eefa191f205d45f00d4a2b36104f0abe95df61182d4

Exchange transactions are usually easily recognizable due to the sheer amount of outputs (and sometimes inputs) they have. Exchange transactions break the transaction graph in a way as the funds that are being sent belong to multiple people and there is no way to tell which customer of the exchange sent funds to which address. People sometimes do use exchanges

as mixers of sorts, but there, of course, exists a big drawback of the exchange itself knowing where users have withdrawn their funds (not to mention being able to freeze the funds if they suspect they have been acquired illegally).

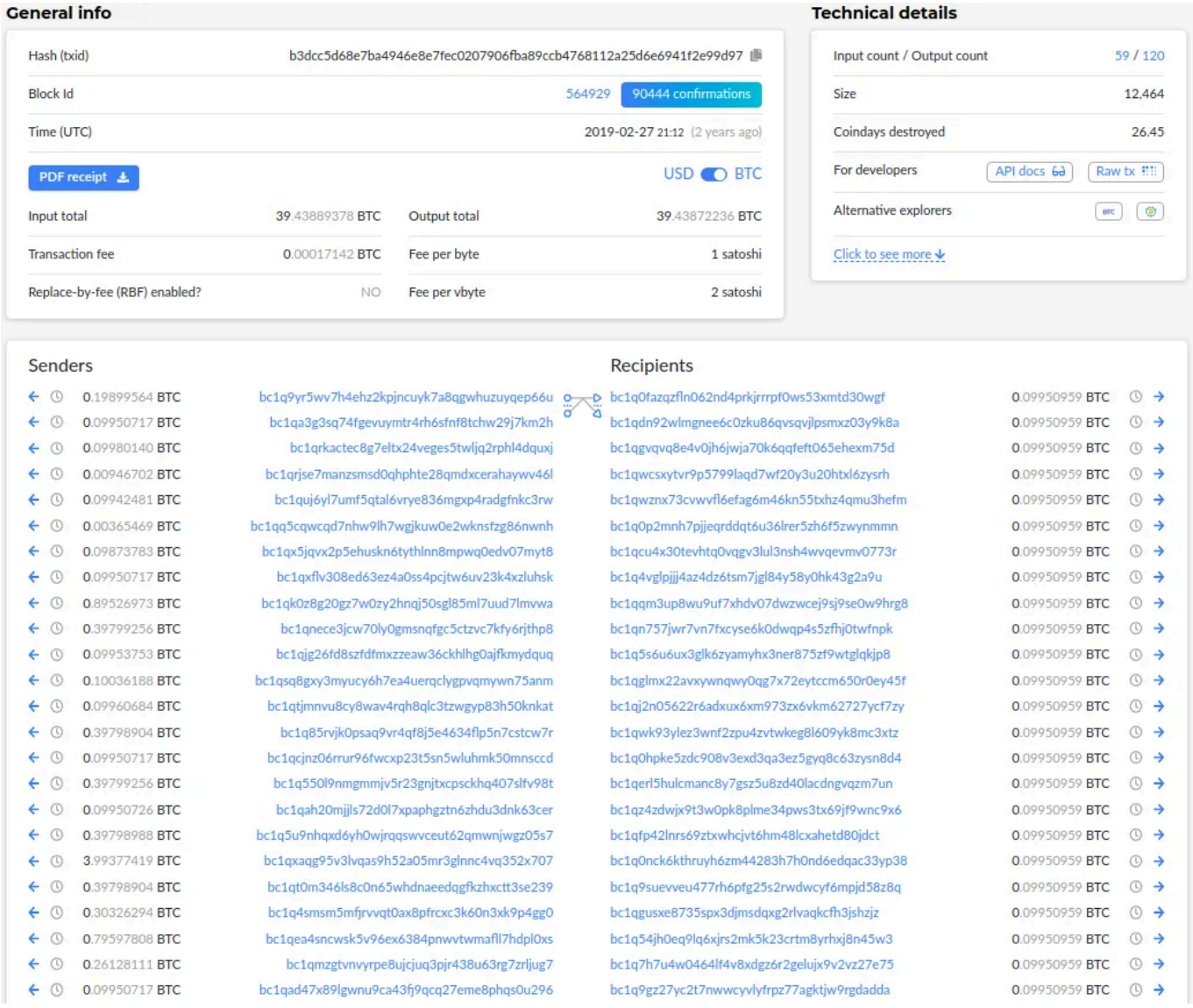
Fun fact, the address 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s belongs to Binance exchange as acknowledged by Binance itself:

John McAfee @officialmcafee · Feb 8, 2018
Replying to @binance @binance_2017 and @cz_binance
Just some questions please: Planned outages are usually announced to a company's user base well in advance. The surprise aspect of yours concerns me. Next, there are screen images - possibly photoshopped - from different people that appear to indicate a hack. Can you comment?
221
67
345
Binance @binance · Feb 8, 2018
Blockchain thankfully provides a public ledger that can disprove any FUD. If you would like to check for yourself, our wallet addresses are:
1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s
0x3f5ce5fbfe3e9af3971dd833d26ba9b5c936f0be
Here you can see we have clearly not been compromised.
297
803
2.8K

https://twitter.com/binance/status/961666467325358081?lang=en

Check it out to see many examples of exchange transactions: https://blockchair.com/bitcoin/address/1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s?_type=address&_search=homepage

> *Coinjoin transactions*



https://blockchair.com/bitcoin/transaction/b3dcc5d68e7ba4946e8e7fec0207906fba89ccb4768112a25d6e6941f2e99d97

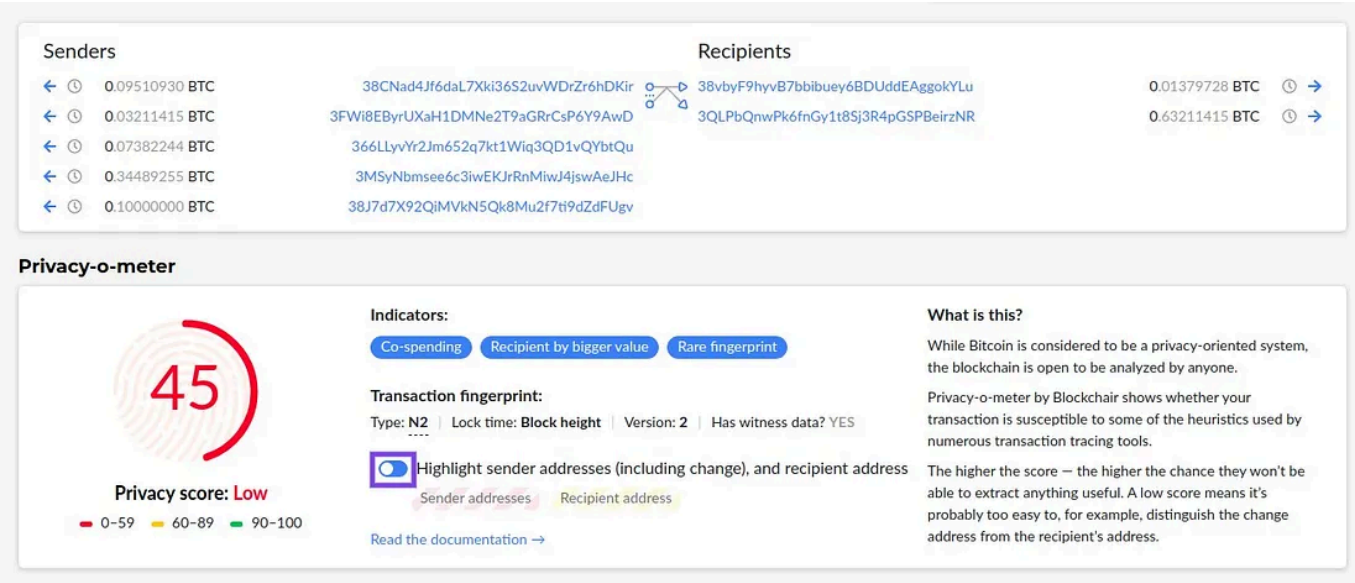
Coinjoins look similar to exchange transactions from the first look, but all their outputs will have the same or very similar amounts (it's worth noting that not all coinjoin transactions have such a high amount of inputs and outputs, but more about a less common type of coinjoins later). Coinjoins truly break the transaction graph as the inputs and outputs belong to different entities and if the coinjoin is constructed correctly (and the entities involved don't make mistakes after the coinjoins is done) there is no way to tell which input is associated with which outputs.

Useful tools

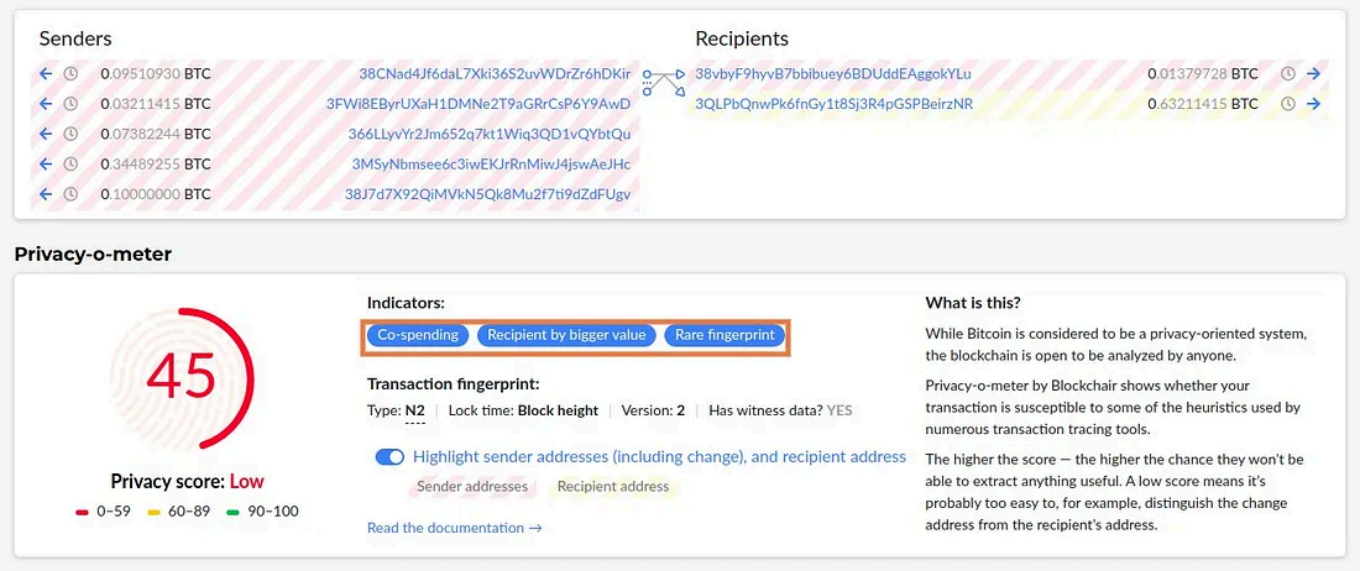
I have scoured the internet for all the free tools that could be of use in forensics investigations. Hopefully, they all still work by the time you are reading this article :D. Feel free to skip this section if you wish and come back when you see me mentioning one of these tools later in the article to get some context.

https://blockchair.com/ — my favorite regular BTC blockchain explorer, although at first glance it is just a regular explorer, but it has very powerful features in the privacy-o-meter tool that automatically determines the likely sender, recipient, and change addresses and it provides a ton of in-depth information about the address such as if it uses RBF, if it has witness data, the next or previous transaction any of the inputs or outputs are involved in (which makes it much easier to follow the path of the funds) and it even has an API, for the nerds :)

You can turn on the privacy-o-meter function by simply toggling this switch:



It will color the sender, receiver, and change addresses in different colors and provide some indications why it thinks that way:



Of course, it's worth noting that you should never blindly trust privacy-o-meter or any other forensics tool. Like everything in blockchain analytics it's built on heuristics (assumptions) which can be wrong. You can read the full list of heuristics privacy-o-meter uses here: https://blockchair.com/api/docs#link_M6

https://blockstream.info/ and https://www.blockchain.com/explorer — alternatives to Blockchair.com you can use that will provide much of the same information but in a bit more technical manner. Blockstream.com and Blockchain.info explorers make it easy to read transaction signatures and Blockstream provides privacy faults of the transaction in a similar way to Blockchair.com explorer (although it provides less information). Of course, you can also use these explorers together.

https://www.kycp.org/#/ — kycp.org is a blockchain explorer created specifically to try to deanonymize coinjoins, it is by far the most powerful

free tool you can use to find links between inputs and outputs in a transaction but it comes with a bit of a learning curve. Explaining the full power of kycp.org is way beyond the scope of this blog, but you can read an explanation by the kycp.org team here: https://medium.com/samourai-wallet/knowing-your-coin-privacy-using-kycp-org-7b3b4385d8b

https://oxt.me/ — this explorer is your best friend when you are exploring the path funds you are following have taken (so-called transaction graph) from the big picture view. Oxt.me has an amazing visualization tool that gives you this ability as well as a wallet clustering feature that automatically clusters addresses into shared wallets. While it's that great to look at individual transactions, it is by far the best tool for wallet clustering and transaction graph visualization (actually, it's the only free tool for transaction graph visualization as far as I'm aware of). It is a must in any investigation.

https://www.walletexplorer.com/ — is an alternative explorer for wallet clustering that you can use instead oxt.me. Walletexplorer.com was created quite a long ago and all in all, it isn't as good as oxt.me at wallet clustering but it has a lot of historical data (it indents old exchange wallets like Mt. Gox and so on) and is certainly worth checking out.

https://learnmeabitcoin.com/tools/path/ — a nifty little tool that tells the shortest path between 2 Bitcoin addresses, sometimes this tool is slow and may be unreliable if the addresses are too far apart, but still can be useful.

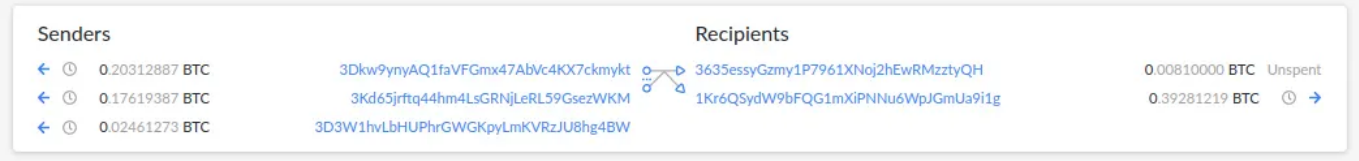
https://bitnodes.io/ — This blog will not be focusing on Bitcoin network surveillance, however, if you were interested in this, the Bitnodes website would probably be the best place to start as it maps out the Bitcoin network by finding all reachable nodes in the network.

https://www.cryptotxalert.com/ — If you find an address you wish to keep an eye on you can use cryptotxalert site to make sure you get an email whenever there is a movement to and/or from that address. Technically this site is paid (though it has a trial for a few weeks) but since the price isn't high and anyone can use the site, it doesn't exactly have a high barrier for entry.

Change address detection

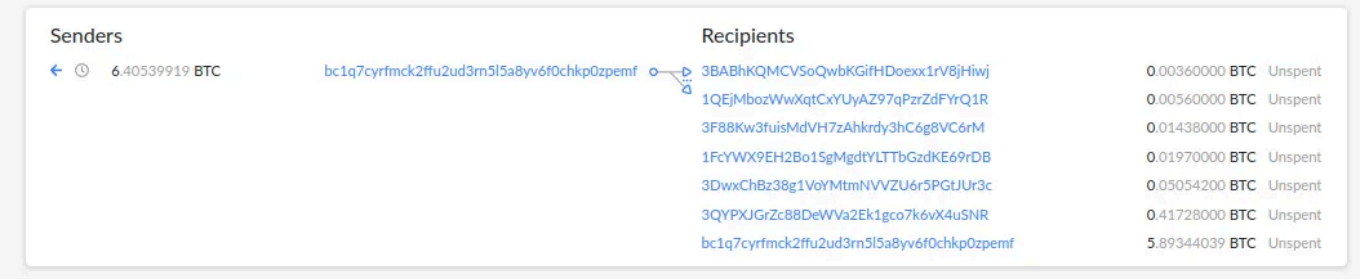
As mentioned before it is not always easy to detect the change address, fortunately, however, there are many clues that can help determine it (although sometimes, it is impossible as well):

- Address reuse — as mentioned, address reuse is horrible for your privacy, especially if the address is reused for change.
- Unnecessary inputs — in the following transaction it is very likely that the address that starts with 363… is the change address while the address starting with 1Kr… is the destination because if the opposite was the case, the transaction would not need to have as many inputs, one would have been enough (although some wallets are badly programmed and take unnecessary inputs for no reason, so take this with a grain of salt):



- Round numbers — if one of the outputs has a round amount (say exactly 1 BTC) it's more likely to be the destination address. The same thing applies when the amount denominated in USD is round (say output was worth exactly 100 USD at the time it was transferred).

- Sending to a different address type — most wallets designate the change address to be the same type as the input addresses, so you may be able to rule out outputs that do not match the input address type.
- Wallet quirks — some wallets will always put the change address first, last, or in some other non-random way.
- Fee bumping — generally, the fee will be bumped from the change address output. If an observant attacker monitors the mempool before the fee was bumped and after they would be able to pick up on which output is the change.
- One of the outputs being vastly bigger than the other — referring to situations like this:



https://blockchair.com/bitcoin/transaction/bf6b6841085d799cf7225d3c1bef1edc854508e51c37e6ecd3f854b2238271b6

- Even without the change address being reused, it would have been obvious it was the change address due to the output being so much bigger than the others. In all likelihood, the other outputs are payouts of some sort.

These are (in my opinion) some of the most important clues, but I'm sure more can be thought of. Some of these clues are more trustworthy then others, it's best to determine a pattern between multiple transactions of entity you're tracking in the blockchain.

Get Pagan's stories in your inbox

Join Medium for free to get updates from this writer.

Enter your email

Subscribe

Remember me for faster sign in

Analyzing metadata

There is a ton of useful metadata that is provided by blockchain explorers about transactions and addresses. It's easy to overlook this information and just focus on the movement of the funds, but important details may be lost that way. For example, if the tracker pays attention to the timestamps on the transactions of the entity they are tracking they may be able to determine the rough timezone the entity in question operates in. Similarly, if the tracker pays attention to the technical characteristics of the transaction (such as fee size, construction of the transaction, scripts, and so on) they may be able to determine what wallet the entity is using as some cryptocurrency wallets are very unique. In general, it is useful to pay attention to any repeating patterns across multiple transactions.

Identifying addresses

Ultimately, the goal of almost all investigations will be to identify the addresses to which the funds in question were sent to or originated from (or both). Doing this is by far the most effective way the target can be de-anonymized, especially if the tracked entity sent their funds to an exchange address. This is of course, especially true for police investigations where law enforcement can reach out to the exchange and order them to provide all the information they have about the suspect. This is so important that, in my

opinion, the number 1 thing you can do to improve your privacy is to make sure you acquire and spend your funds in a KYC-less way, for example, try acquiring Bitcoins via a peer-to-peer exchange such as LocalBitcoins, instead of a regular centralized exchange. More information on how that can be done can be found here: https://www.buybitcoinworldwide.com/kb/buy-bitcoin-without-verification-id/

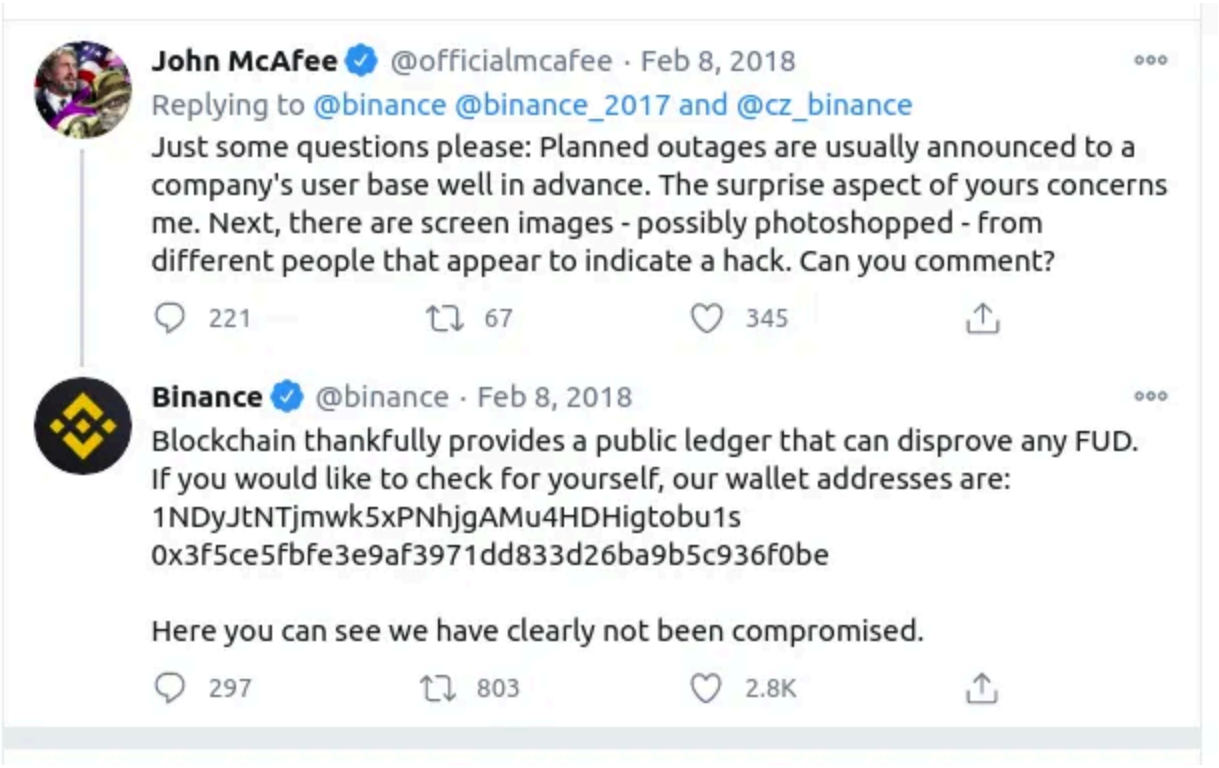
Understanding that you came across an exchange address isn't difficult, exchange addresses will usually have a very high count of very frequent transactions. Here are a few examples:

- https://blockchair.com/bitcoin/address/1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s
- https://blockchair.com/bitcoin/address/3Cbq7aT1tY8kMxWLbitaG7yT6bPbKChq64
- https://blockchair.com/bitcoin/address/12cgpFdJViXbwHbhrA3TuW1EGnL25Zqc3P

Identifying to which exact exchange they belong is the hard part. There are a few things you can try to do that:

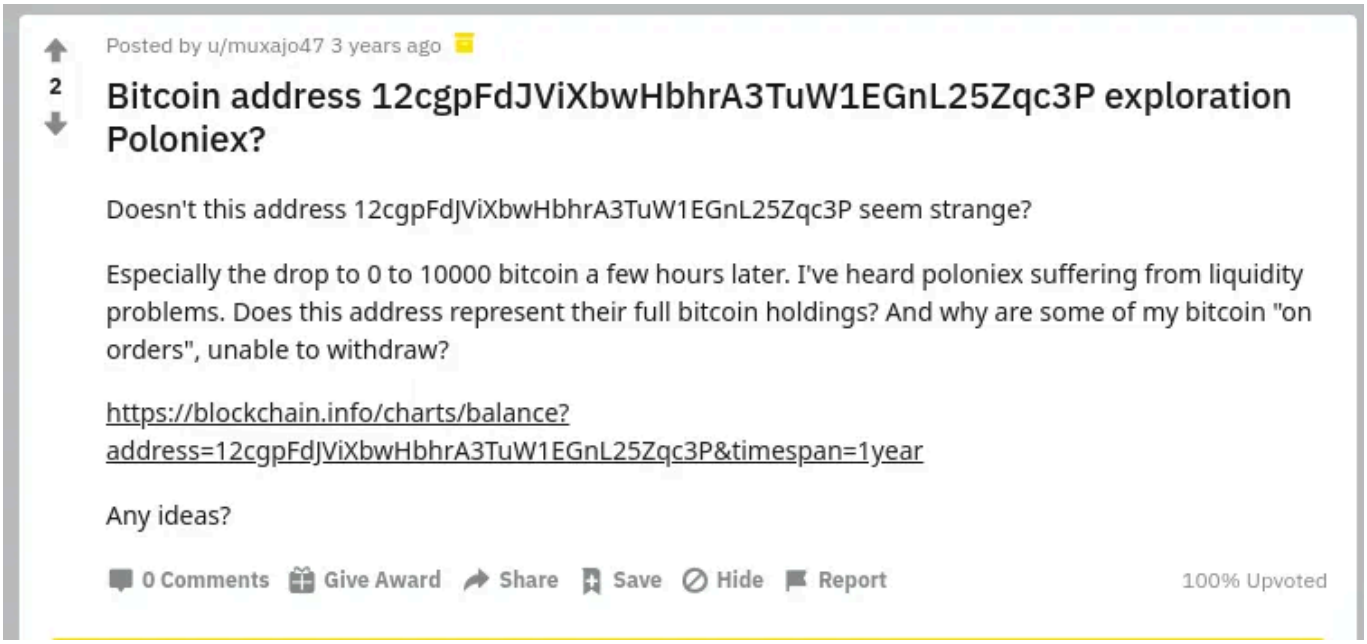
> *Just try googling the address…*

If the address you are trying to identify belongs to a large enough exchange someone has bound to have mentioned the address somewhere on the internet. You may not always be lucky enough to find tweets from official exchange accounts mentioning their address:


John McAfee @officialmcafee · Feb 8, 2018
Replying to @binance @binance_2017 and @cz_binance
Just some questions please: Planned outages are usually announced to a company's user base well in advance. The surprise aspect of yours concerns me. Next, there are screen images - possibly photoshopped - from different people that appear to indicate a hack. Can you comment?
221
67
345
Binance @binance · Feb 8, 2018
Blockchain thankfully provides a public ledger that can disprove any FUD. If you would like to check for yourself, our wallet addresses are:
1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s
0x3f5ce5fbfe3e9af3971dd833d26ba9b5c936f0be
Here you can see we have clearly not been compromised.
297
803
2.8K

https://twitter.com/binance/status/961666467325358081?lang=en

But finding a Reddit post from a disgruntled exchange customer is completely realistic:


Posted by u/muxajo47 3 years ago
2
Bitcoin address 12cgpFdJViXbwHbhrA3TuW1EGnL25Zqc3P exploration Poloniex?
Doesn't this address 12cgpFdJViXbwHbhrA3TuW1EGnL25Zqc3P seem strange?
Especially the drop to 0 to 10000 bitcoin a few hours later. I've heard poloniex suffering from liquidity problems. Does this address represent their full bitcoin holdings? And why are some of my bitcoin "on orders", unable to withdraw?
https://blockchain.info/charts/balance?address=12cgpFdJViXbwHbhrA3TuW1EGnL25Zqc3P&timespan=1year
Any ideas?
0 Comments
Give Award
Share
Save
Hide
Report
100% Upvoted

https://www.reddit.com/r/CryptoCurrency/comments/6ind8l/bitcoin_address/

Obviously, Reddit and other social media posts aren't as strong evidence as tweets from the official Twitter account of the exchange but it can be something to hold on to.

When googling the address you may want to enter the address together with "-block" command. This will automatically remove all search results that have the word "block" in their URL, so most blockchain explorers would simply show the address without providing any information about it.

> *Try using block explorers which index famous addresses…*

Some blockchain explorers actually attempt to index known exchange addresses and/or wallets, none of them are close to complete, but it's certainly worth searching them. Here are a few of these explorers -

- https://oxt.me/
- https://www.walletexplorer.com/
- https://www.bitcoinabuse.com/
- https://bitinfocharts.com/
- https://vivigle.com/
- https://checkbitcoinaddress.com/

Outro

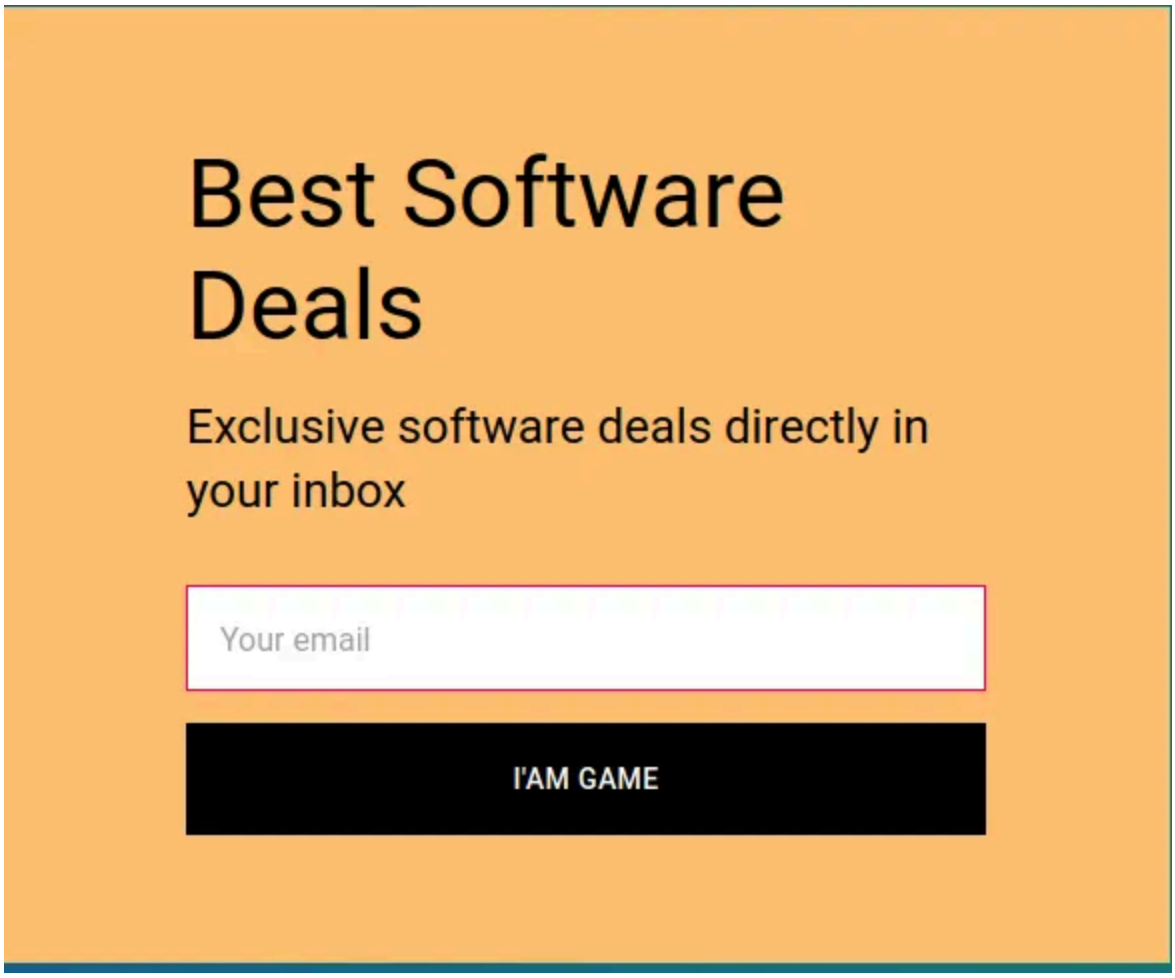
This concludes part 1 of the 3 part series, in the next part we will explore more complex concepts that are very helpful to know in Bitcoin analytics such as address formats, transaction graph, wallet guestimation and fingerprinting, coinjoins, payjoins, and more.

Also, Read

- Crypto Trading Bots
- Uniswap API — How to get Uniswap data?
- AAX Exchange Review | Referral Code, Trading Fee, Pros and Cons
- Deribit Review | Options, Fees, APIs and Testnet
- FTX Crypto Exchange Review
- Bybit Exchange Review
- The Best Bitcoin Hardware wallet
- Crypto Copy Trading Platforms
- Bitsgap vs 3Commas vs Quadency
- The Best Crypto Tax Software
- Best Crypto Trading Platforms
- Best Crypto Lending Platforms
- Ledger Nano S vs Trezor one vs Trezor T vs Ledger Nano X
- BlockFi vs Celsius vs Hodlnaut
- Bitsgap review — A Crypto Trading Bot That Makes Easy Money
- Quadency Review- A Crypto Trading Bot Made For Professionals
- PrimeXBT Review | Leverage Trading, Fee and Covesting
- Altrady review
- Ellipal Titan Review
- SecuX Stone Review
- BlockFi Review | Earn up to 8.6% interests on your Crypto

- Best Crypto APIs for Developers
- Best Blockchain Analysis Tools
- Crypto arbitrage guide: How to make money as a beginner
- Top Bitcoin Node Providers
- Best Crypto Charting Tool
- What are the best books to learn about Bitcoin?

Get Best Software Deals Directly In Your Inbox



Bitcoin Cryptocurrencie Forensics Analytics Blockchain

Published in Coinmonks

144K followers · Last published 8 hours ago

Follow

Coinmonks is a non-profit Crypto Educational Publication. Other Project—https://coincodecap.com/ & Email—gaurav@coincodecap.com

Written by Pagan

30 followers · 37 following

Follow

Just a hobbyist crypto enthusiast :)

No responses yet

Write a response

What are your thoughts?

More from Pagan and Coinmonks

Pagan · Feb 19

Book Reviews — Governance and Civics

Disclaimer — I'm writing this and other posts on this blog mostly to document my own...

In Coinmonks by Johnwege · Jun 29

The Deathblow Has Finally Been Dealt to Bitcoin?

Perhaps this time, Bitcoin won't recover.

490 28 2

In Coinmonks by Joseph Orefice · Jun 7

I Asked Four AIs How Bitcoin Falls to $1,000 or Less

A few weeks ago I asked four AIs the million-dollar question. This is the other one — the...

449 18 2

In Coinmonks by Pagan · Jun 15, 2021

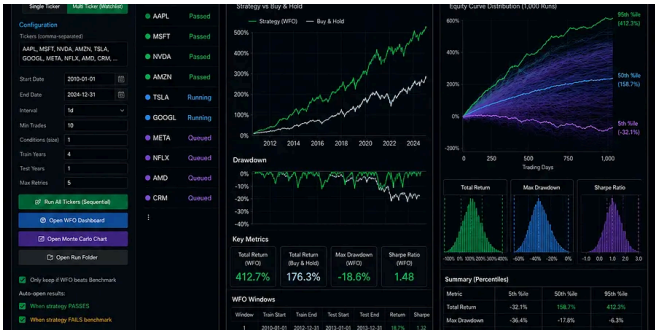
Free Bitcoin Forensics - Part 3

Greetings and welcome to the 3rd and final part of the "Free Bitcoin Forensics" blog...

81

See all from Pagan See all from Coinmonks

Recommended from Medium



Kryptera · Jun 17

I Built a Desktop App That Automatically Discovers Trading...

The Python bundle worked. But it wasn't for everyone. So I fixed that.

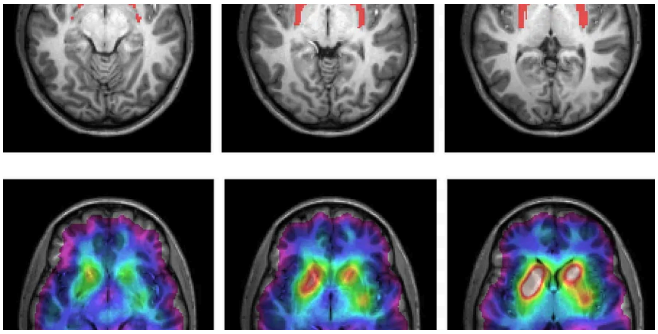
126 1 2

```
[toolchain]
package_manager = "yarn"

[features]
resolution = true
skip-lint = false

[programs.devnet]
solana_accounts = "Ga1UVR2AoZAazWCSZQUg7ZdKkpNXxLCXju4eN5YRrKQJ"

[registry]
url = "https://api.apr.dev"

[provider]
cluster = "devnet"
wallet = "~/.config/solana/id.json"

[scripts]
test = "yarn run ts-mocha -p ./tsconfig.json -t 1000000 tests/**/*.ts"
```

Andrey Obruchkov · Apr 22

Understanding Anchor Accounts: Seeds, Bumps, PDAs, and How th...

When you start building on Solana with Anchor, the hardest part isn't Rust it's...



In Write A Catal... by Dr. Patricia Schmidt... · Jan 14

As a Neuroscientist, I Quit These 5 Morning Habits That Destroy You...

Most people do #1 within 10 minutes of waking (and it sabotages your entire day)

59K 1356 546

Sips & Scale · May 13

The Only Polymarket Strategies I Trust

Why the real edge starts with execution

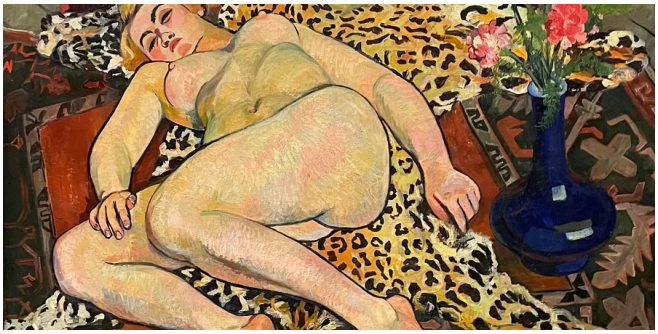
158

Mona Lazar · Jun 8

5 Assets Every Adult Should Own (And Most Never Do)

We work our whole life for others and end up owning nothing that works for us

8.1K 208 66



Richard Krueger · Apr 1

Marriage, Affairs, and the Problem No One Talks About

About a year and a half ago, my wife — whom I've been married to for forty years — had an...

17.2K 540 67

See more recommendations